CLAIMS

What is Claimed is:

1. A method of storing program material for subsequent replay, comprising the steps of:

receiving access control information and the program material encrypted according to a first encryption key, the access control information including the first encryption key and control data;

further encrypting the access control information and the encrypted program material according to a second encryption key;

encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; and

storing the encrypted access control information and encrypted program material and the fourth encryption key.

2. The method of claim 1, further comprising the steps of:

reading the further encrypted access control information and encrypted program material and the fourth encryption key;

decrypting the further encrypted access control information to produce the encrypted access control information;

decrypting the fourth encryption key using the third encryption key to produce the second encryption key;

decrypting the encrypted access control information to produce the first encryption key; and

decrypting the program material using the first encryption key.

3. The method of claim 2, wherein

the access control information further comprises data describing a right associated with the program material; and

the steps of decrypting the encrypted access control information to produce the first encryption key and decrypting the program material using the first encryption key is performed according to the data describing the right.

4. The method of claim 3, wherein the right is expressed in a metadata table.

5. The method of claim 4, wherein the metadata table comprises data selected from the group comprising:

at least one default value wherein the data describing a right associated with the program material comprises a change to at least one of the default values; and

at least one control value expressing a condition that must be satisfied before pre-cached program material is presented to the subscriber.

6. The method of claim 3, wherein the right is selected from the group comprising:

a storage right;

a viewing right, having at least one viewing right characteristic selected from the group comprising:

a non-purchase lifetime of the program material;

a lifetime of the program material after a purchase of the program material;

a number of permitted views per purchase of the program material;

a cost to repurchase the program material; and

a number of permitted views per repurchase of the program material.

7. The method of claim 2, further comprising the step of providing the decrypted program material to a presentation device.

8. The method of claim 2, further comprising the steps of:

storing the decrypted program material; and

reading the decrypted program material according to a user command.

9. The method of claim 8, wherein the user command is selected from the group comprising:

a play command;

a rewind command;

a fast forward command;

a fast reverse play command;

a fast forward play command;

a pause command;

a frame step command; and

a stop command.

10. The method of claim 2, further comprising the steps of:

re-encrypting the decrypted program material according to the second encryption key;

encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; and

storing the re-encrypted program material and the fourth encryption key.

11. The method of claim 10, wherein:

the access control information further comprises data describing viewing rights for the program material; and

the steps of decrypting the encrypted access control information to produce the first encryption key and decrypting the program material using the first encryption key is performed according to the data describing the viewing rights.

12. The method of claim 11, further comprising the steps of:

reading the re-encrypted program material and the fourth encryption key;

decrypting the fourth encryption key with the third key to produce the second encryption key; and

decrypting the program material using the second encryption key.

13. The method of claim 12, further comprising the step of providing the decrypted program material to a presentation device.

14. The method of claim 12, wherein the steps of reading the re-encrypted program material and the fourth encryption key, decrypting the fourth encryption key with the third encryption key to produce the second encryption key, and decrypting the program material using the second encryption key are performed according to a user command.

15. The method of claim 14, wherein the user command is selected from the group comprising:

a play command;

a rewind command;

a fast forward command;

a fast reverse play command;

a fast forward play command;

a pause command;

a frame step command; and

a stop command.

16. An apparatus for storing program material for subsequent replay, comprising:

a tuner, for receiving encrypted access control information and the program material encrypted according to a first encryption key, the access control information including the first encryption key and control data;

a first encryption module, communicatively coupled to the tuner and communicatively coupleable to a data storage device, the first encryption module for further encrypting the encrypted program material and the access control information according to a second encryption key;

a second encryption module, communicatively coupled to the first encryption module and communicatively coupleable to the data storage device, the second encryption module for encrypting the second encryption key according to a third encryption key to produce a fourth encryption key;

a first decryption module, communicatively coupleable to the disk drive, for decrypting the fourth encryption key to produce the second encryption key;

a second decryption module, communicatively coupled to the first decryption module and the tuner and communicatively coupleable to the data storage device, for decrypting the further encrypted program material to produce the encrypted program material and the encrypted access control information using the second encryption key;

a conditional access module, communicatively coupleable to the second decryption module and the tuner, for selectably accepting the access control information selected from the group comprising the access control information received in the tuner and the access control information decrypted by the second decryption module, the conditional access module comprising a third decryption module for decrypting the encrypted access control information to produce the first encryption key; and

a fourth decryption module for decrypting the encrypted program material to produce unencrypted program material using the first encryption key.

17. The apparatus of claim 16, further comprising:

a third encryption module, communicatively coupled to the fourth decryption module and communicatively coupleable to a second media storage device, the third encryption module for encrypting the unencrypted program material according to the second encryption key; and

a fifth decryption module, communicatively coupleable to the second media storage device, for decrypting the encrypted program material using the second encryption key.

18. The apparatus of claim 17, wherein the third encryption module encrypts the unencrypted program material and provides the encrypted program material to the data storage device when a subscriber selects a trick play operation

19. The apparatus of claim 17, wherein the third encryption module encrypts the unencrypted program material and provides the encrypted program material to the data storage device when the subscriber purchases the program material.

20. The apparatus of claim 16, wherein:

the fourth decryption module is communicatively coupled to the first encryption module; and

the second decryption module is communicatively coupleable to a presentation device.

21. The apparatus of claim 20, wherein:

the first encryption module encrypts the unencrypted program material using the second encryption key, and provides the encrypted program material to the data storage device; and

the second decryption module accepts the encrypted program material from the data storage device and decrypts the encrypted program material using the second encryption key.

22. The apparatus of claim 16, further comprising the data storage device, for storing and retrieving the further encrypted program materials and the fourth encryption key.

23. The apparatus of claim 16, wherein the third decryption module is implemented in a smartcard.

24. The apparatus of claim 16, wherein the control data is temporally variant.

25. An apparatus for storing program material for subsequent replay, comprising:

means for receiving access control information and the program material encrypted according to a first encryption key, the access control information including the first encryption key and control data;

means for further encrypting the access control information and the encrypted program material according to a second encryption key;

means for encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; and

means for storing the encrypted access control information and encrypted program material and the fourth encryption key.

A

30

26. The apparatus of claim 25, further comprising:

means for retrieving the further encrypted access control information and encrypted program material and the fourth encryption key;

means for decrypting the further encrypted access control information to produce the encrypted access control information;

means for decrypting the fourth encryption key using the third encryption key to produce the second encryption key;

means for decrypting the encrypted access control information to produce the first encryption key; and

means for decrypting the program material using the first encryption key.

27. The apparatus of claim 26, wherein:

the access control information further comprises data describing at least one right for the program material; and

encrypted access control information the encrypted program material is decrypted according to the data describing the right.

28. The apparatus of claim 27, wherein the right is selected from the group comprising:

a storage right;

a viewing right, having at least one viewing right characteristic selected from the group comprising:

a non-purchase lifetime of the program material;

a lifetime of the program material after a purchase of the program material;

a number of permitted views per purchase of the program material;

a cost to repurchase the program material; and

a number of permitted views per repurchase of the program material.

29. The apparatus of claim 26, further comprising means for providing the decrypted program material to a presentation device.

30. The apparatus of claim 26, further comprising:

means for storing the decrypted program material; and

means for retrieving the decrypted program material according to a user command.

31. The apparatus of claim 30, wherein the user command is selected from the group comprising:

a play command;

a rewind command;

a fast forward command;

a fast reverse play command;

a fast forward play command;

a pause command;

a frame step command; and

a stop command.

32. The apparatus of claim 26, further comprising:

means for re-encrypting the decrypted program material according to the second encryption key;

means for encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; and

means for storing the re-encrypted program material and the fourth encryption key.

33. The apparatus of claim 32, wherein:

the access control information further comprises data describing at least one right for the program material; and

encrypted access control information the encrypted program material is decrypted according to the data describing the right.

34. The apparatus of claim 33, further comprising:

means for reading the re-encrypted program material and the fourth encryption key;

means for decrypting the fourth encryption key with the third key to produce the second encryption key; and

means for decrypting the program material using the second encryption key.

35. The apparatus of claim 34, further comprising means for providing the decrypted program material to a presentation device.

36. The apparatus of claim 34, wherein the re-encrypted program material and the fourth encryption key is read, the fourth decryption key is decrypted with the third key to produce the second encryption key, and the program material is decrypted using the second decryption key according to a user command.

37. The apparatus of claim 36, wherein the user command is selected from the group comprising:

a play command;
a rewind command;
a fast forward command;
a fast reverse play command;
a fast forward play command;
a pause command;
a frame step command; and
a stop command.